WHAT IS CLAIMED IS:

1. A distributed digital signature generation method for generating a digital signature for a digital document by using a plurality of partial digital signature generation parts, said distributed digital signature generation method comprising the steps of:

each of said partial digital signature generation parts generating a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generating a partial digital signature by using said partial signature key for a hash value of an input digital document;

each of said partial digital signature generation parts outputting said partial digital signature or a pair of said digital document and said partial digital signature;

combining a predetermined number of partial digital signatures generated by said partial digital signature parts wherein said predetermined number is a threshold;

performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of partial digital signatures; and

generating an integrated digital signature from a result of said transformation process.

2. The distributed digital signature generation method as claimed in claim 1, wherein a

least common multiple of predetermined values is used as a transformation number in said transformation process.

3. The distributed digital signature generation method as claimed in claim 1, said method further comprising the step of:

judging whether an incorrect partial digital signature generated by an incorrect partial signature key exists, and identifying said incorrect partial digital signature by combining said predetermined number of said partial digital signatures and performing a signature verification process.

4. A distributed digital signature generation method for generating a digital signature for a digital document by using a plurality of partial digital signature generation parts, said method comprising the steps of:

each of said partial digital signature generation parts adding one or more items of additional information to an input digital document to generate a digital document with additional information;

each of said partial digital signature generation parts generating a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generating a partial digital

signature by using said partial signature key for a hash value of said digital document with additional information;

each of said partial digital signature generation parts outputting a pair of said digital document with additional information and said partial digital signature;

combining a predetermined number of said pairs of said digital document with additional information and said partial digital signature wherein said predetermined number is a threshold;

performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of pairs; and

generating an integrated digital signature from a result of said transformation process.

5. The distributed digital signature generation method as claimed in claim 5, wherein a least common multiple of predetermined values is used as a transformation number in said transformation process.

6. The distributed digital signature generation method as claimed in claim 4, said method further comprising the step of:

judging whether an incorrect partial digital signature generated by an incorrect partial signature key exist and identifying said incorrect partial digital signature by combining said

predetermined number of said partial digital signatures and performing a signature verification process.

7. A distributed digital signature generation apparatus for generating a digital signature for a digital document by using a plurality of partial digital signature generation parts, wherein:

each of said partial digital signature generation parts generates a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generates a partial digital signature by using said partial signature key for a hash value of an input digital document;

each of said partial digital signature generation parts outputs said partial digital signature or a pair of said digital document and said partial digital signature;

said distributed digital signature generation apparatus comprising:

a part for combining a predetermined number of partial digital signatures generated by said partial digital signature parts wherein said predetermined number is a threshold;

a part for performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of partial digital signatures; and

a part for generating an integrated digital signature from a result of said

transformation process.

8. The distributed digital signature generation apparatus as claimed in claim 7, wherein a least common multiple of predetermined values is used as a transformation number in said transformation process.

9. The distributed digital signature generation apparatus as claimed in claim 7, said apparatus further comprising:

a part for judging whether an incorrect partial digital signature generated by an incorrect partial signature key exists and identifying said incorrect partial digital signature by combining said predetermined number of said partial digital signatures and performing a signature verification process.

10. A distributed digital signature generation apparatus for generating a digital signature for a digital document by using a plurality of partial digital signature generation parts, wherein:

each of said partial digital signature generation parts adds one or more items of additional information to an input digital document to generate a digital document with additional

information;

each of said partial digital signature generation parts generates a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generates a partial digital signature by using said partial signature key for a hash value of said digital document with additional information;

each of said partial digital signature generation parts outputs a pair of said digital document with additional information and said partial digital signature;

said distributed digital signature generation apparatus comprising:

a part for combining a predetermined number of said pairs of said digital document with additional information and said partial digital signature wherein said predetermined number is a threshold;

a part for performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of pairs; and

a part for generating an integrated digital signature from a result of said transformation process.

11. The distributed digital signature generation apparatus as claimed in claim 10, wherein a least common multiple of predetermined values is used as a transformation number in said transformation process.

12. The distributed digital signature generation apparatus as claimed in claim 10, said apparatus further comprising:

a part for judging whether an incorrect partial digital signature generated by an incorrect partial signature key exists and specifying said incorrect partial digital signature by combining said predetermined number of said partial digital signatures and performing a signature verification process.

13. A digitally signed digital document generation method for generating a digital document with a digital signature generated by using a plurality of partial digital signature generation parts, said digitally signed digital document generation method comprising the steps of:

each of said partial digital signature generation parts generating a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generating a partial digital signature by using said partial signature key for a hash value of an input digital document;

each of said partial digital signature generation parts outputting said partial digital signature or a pair of said digital document and said partial digital signature;

combining a predetermined number of

partial digital signatures generated by said partial digital signature parts wherein said predetermined number is a threshold;

performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of partial digital signatures;

generating an integrated digital signature from a result of said transformation process; and

generating a digital document with digital signature which includes said digital document and said integrated digital signature.

14. A digitally signed digital document generation method for generating a digital document with a digital signature generated by using a plurality of partial digital signature generation parts, said digitally signed digital document generation method comprising the steps of:

each of said partial digital signature generation parts adding one or more items of additional information to an input digital document to generate a digital document with additional information;

each of said partial digital signature generation parts generating a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generating a partial digital signature by using said partial signature key for a hash value of said digital document with additional information;

each of said partial digital signature

generation parts outputting a pair of said digital document with additional information and said partial digital signature;

combining a predetermined number of said pairs of said digital document with additional information and said partial digital signature wherein said predetermined number is a threshold;

performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of pairs; and

generating an integrated digital signature from a result of said transformation process; and

generating a digital document with digital signature which includes said digital document and said integrated digital signature.

15. A digitally signed digital document generation apparatus for generating a digital document with a digital signature generated by using a plurality of partial digital signature generation parts, wherein:

each of said partial digital signature generation parts generates a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generates a partial digital signature by using said partial signature key for a hash value of an input digital document;

each of said partial digital signature generation parts outputs said partial digital signature or a pair of said digital document and said partial digital signature;

said digitally signed digital document generation apparatus comprising:

a part for combining a predetermined number of partial digital signatures generated by said partial digital signature parts wherein said predetermined number is a threshold;

a part for performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of partial digital signatures;

a part for generating an integrated digital signature from a result of said transformation process; and

a part for generating a digital document with digital signature which includes said digital document and said integrated digital signature.

16. A digitally signed digital document generation apparatus for generating a digital document with a digital signature generated by using a plurality of partial digital signature generation parts, wherein:

each of said partial digital signature generation parts adds one or more items of additional information to an input digital document to generate a digital document with additional information;

each of said partial digital signature generation parts generates a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generates a partial digital

signature by using said partial signature key for a hash value of said digital document with additional information;

each of said partial digital signature generation parts outputs a pair of said digital document with additional information and said partial digital signature;

said digitally signed digital document generation apparatus comprising:

a part for combining a predetermined number of said pairs of said digital document with additional information and said partial digital signature wherein said predetermined number is a threshold;

a part for performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of pairs;

a part for generating an integrated digital signature from a result of said transformation process; and

a part for generating a digital document with digital signature which includes said digital document and said integrated digital signature.

17. A program for causing a computer to generate a digital signature for a digital document by using a plurality of partial digital signature generation parts, wherein:

each of said partial digital signature generation parts generates a partial signature key by communicating with each other without using a

trusted third party;

each of said partial digital signature generation parts generates a partial digital signature by using said partial signature key for a hash value of an input digital document;

each of said partial digital signature generation parts outputs said partial digital signature or a pair of said digital document and said partial digital signature;

said program comprising:

program code means for combining a predetermined number of partial digital signatures generated by said partial digital signature parts wherein said predetermined number is a threshold;

program code means for performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of partial digital signatures; and

program code means for generating an integrated digital signature from a result of said transformation process.

18. A program for causing a computer to generate a digital signature for a digital document by using a plurality of partial digital signature generation parts, wherein:

each of said partial digital signature generation parts adds one or more items of additional information to an input digital document to generate a digital document with additional information;

each of said partial digital signature generation parts generates a partial signature key

by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generates a partial digital signature by using said partial signature key for a hash value of said digital document with additional information;

each of said partial digital signature generation parts outputs a pair of said digital document with additional information and said partial digital signature;

said program comprising:

program code means for combining a predetermined number of said pairs of said digital document with additional information and said partial digital signature wherein said predetermined number is a threshold;

program code means for performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of pairs; and

program code means for generating an integrated digital signature from a result of said transformation process.

19. A computer readable medium storing program code for causing a computer to generate a digital signature for a digital document by using a plurality of partial digital signature generation parts, wherein:

each of said partial digital signature generation parts generates a partial signature key

by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generates a partial digital signature by using said partial signature key for a hash value of an input digital document;

each of said partial digital signature generation parts outputs said partial digital signature or a pair of said digital document and said partial digital signature;

said computer readable medium comprising:

program code means for combining a predetermined number of partial digital signatures generated by said partial digital signature parts wherein said predetermined number is a threshold;

program code means for performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of partial digital signatures; and

program code means for generating an integrated digital signature from a result of said transformation process.

20. A computer readable medium storing program code for causing a computer to generate a digital signature for a digital document by using a plurality of partial digital signature generation parts, wherein:

each of said partial digital signature generation parts adds one or more items of additional information to an input digital document to generate a digital document with additional information;

each of said partial digital signature generation parts generates a partial signature key by communicating with each other without using a trusted third party;

each of said partial digital signature generation parts generates a partial digital signature by using said partial signature key for a hash value of said digital document with additional information;

each of said partial digital signature generation parts outputs a pair of said digital document with additional information and said partial digital signature;

said computer readable medium comprising:

program code means for combining a predetermined number of said pairs of said digital document with additional information and said partial digital signature wherein said predetermined number is a threshold;

program code means for performing a transformation process on each of said predetermined number of partial digital signatures according to combination of said predetermined number of pairs; and

program code means for generating an integrated digital signature from a result of said transformation process.